Une caractérisation non gaussienne et à longue mémoire du trafic Internet et de ses anomalies : validation expérimentale et application à la détection d'attaque de DDoS

P. Borgnat, P. Abry, G. Dewaele[1], A. Scherrer[2], N. Larrieu, P. Owezarski, Y. Labit[3], L. Gallon, J. Aussibal[4]

[1] Laboratoire de physique, UMR 5672 CNRS, ENS de Lyon. [2] LIP, UMR 5668 CNRS, INRIA, ENS de Lyon. [3] LAAS-CNRS, UPR 8001, Toulouse. [4] Laboratoire d'informatique de Pau et des Pays de l'Adour, IUT de Mont de Marsan

Rançon de son succès, l'Internet est victime d'anomalies de trafic (pannes, augmentations soudaines, attaques). Pour comparer les statistiques du trafic régulier avec celles en situation anormale, nous menons des campagnes de mesures collectant du trafic régulier et du trafic contenant des anomalies. Ces mesures sont effectuées sur le réseau RENATER par le projet METROSEC, en produisant des anomalies de type dénis de service (DoS) à partir de logiciels d'attaque réels (TFN2K, TRIN00) visant différents services (ICMP, SYN, UDP, TCP), ou des anomalies de « foules subites ». Nous introduisons un modèle de trafic multirésolution, non gaussien et à mémoire longue et les estimateurs adéquats. Le modèle décrit à tous les niveaux d'agrégation tant le trafic normal que du trafic avec anomalies. Nous montrons qu'il permet de détecter si des anomalies sont présentes ou non et si ces anomalies sont dues à des foules subites ou à des attaques DoS.

Being now a mainstream communication, the Internet is subject to many kinds of anomalies (failures, flash-crowds, attacks). In order to compare the statistics of normal traffic with traffic with anomalies, we collect both regular and anomalous traffic. The traffic is collected on the RENATER *network by the* METROSEC *project and we produce both Denial of Service (DoS) attacks with real attack softwares (TFN2K, TRIN00) aimed at various services (ICMP, SYN, UDP, TCP), and flash-crowd anomalies. We propose a multiresolution, non-Gaussian model with long memory and the corresponding estimators. It models, jointly at all aggregation levels, normal traffic, and also traffic containing anomalies. We show that the model enables to detect the anomalies in the traffic and distinguish between flash-crowd and DoS types of anomaly.*

Mots-clés : attaques DoS, foules subites, processus non gaussiens, longue mémoire, détection d'anomalies.
Keywords : *DoS attacks, Floash Crowds, Non-Gaussian processus, Long Memory, Anomaly Detection.*

I Motivation

L'Internet est devenu le réseau de communication universel pour tous les types d'informations, du transfert simple de fichiers binaires à la transmission de la voix, de la vidéo, d'informations interactives en temps réel,... L'Internet doit donc évoluer d'une offre de service *best effort* unique vers une offre multi-services, ce qui le rend du coup plus sensible aux attaques, en particulier les attaques de dénis de service simples ou distribuées. En effet, les attaques DoS (*Denial of Service*) modifient les caractéristiques du trafic, pouvant par exemple réduire de façon significative le niveau de qualité de service (QoS) perçu par les utilisateurs du réseau. Cela peut entraîner une violation des SLA (*Service Level Agreement*) à la charge du founisseur d'accès (ISP) et de lourdes pertes financières pour ce dernier.

Combattre les attaques DoS est une tâche difficile et les systèmes de détection d'intrusion (IDS), notamment ceux basés sur la détection d'anomalies, ne sont pas très efficaces. En premier lieu, les IDS sont limités par la multitude de formes que peuvent prendre les attaques DoS, rendant difficile une définition

unique de ces attaques. De surcroît, l'évolution actuelle de l'Internet (multiplication des types de trafics) rend plus délicate la définition de ce qu'est le trafic normal et donc la conception d'un IDS efficace. Il est observé en particulier que le trafic Internet présente en soi une variabilité très forte en situation de trafic normal, et ce quelle que soit l'échelle de temps de surveillance [39]. Ces propriétés sont décrites en terme de longue mémoire [16], d'auto-similarité [40] ou multifractalité [19]. Elles rendent plus délicate et incertaine la détection d'anomalies. Finalement, le trafic Internet peut subir des variations globales fortes, soudaines mais légitimes (comme des foules subites – ou *flash crowds* en anglais (FC) – par exemple) qu'il peut être difficile de distinguer des variations illégitimes. Pour ces raisons, les IDS basés sur la détection d'anomalies par profil statistique souffrent souvent de taux élevés de faux positifs et sont peu populaires.

Le présent travail, réalisé dans le cadre du projet METROSEC [43] (projet de l'ACI Sécurité & Informatique, 2004-2007) a pour objectifs principaux d'analyser l'impact des anomalies sur les caractéristiques statistiques et de mettre en évidence des signatures caractéristiques du trafic contenant des anomalies légitimes (par exemples des foules subites) et illégitimes (attaques DDoS,...). La finalité de ces résultats est de servir de base pour améliorer les mécanismes réseau en les rendant capables de réagir aux anomalies.

À ces fins, nous proposons de modéliser le trafic internet à l'aide d'un modèle de processus stochastique non gaussien et à mémoire longue. Nous montrons expérimentalement que ce modèle est suffisamment versatile pour décrire une grande variété de trafics réguliers ainsi que des trafics comportant des anomalies, légitimes ou non. Nous montrons que les évolutions des paramètres estimés pour ce modèle permettent de différencier le trafic avec et sans anomalie et de classifier les anomalies. Ces démonstrations expérimentales utilisent des traces de trafic capturées sur une plate-forme de métrologie de l'Internet, mise en place sur le réseau RENATER dans le cadre du projet METROSEC. Cette plate-forme nous a permis d'abord d'enregistrer régulièrement du trafic normal, puis de conduire des expériences pour capturer des traces contenant des anomalies. Pour cela, nous avons généré des anomalies contrôlées et reproductibles (ce qui est essentiel pour la validation du modèle et des méthodes de détection d'intrusion qui vont en découler). Nous disposons ainsi d'une base de données de traces de trafic contenant des anomalies documentées.

La partie II décrit la production et le contenu de cette base de données de traces avec et sans anomalies. La partie III présente les processus Gamma-farima, employés comme modèle non gaussien et à longue mémoire pour caractériser le trafic. Nous validons ce modèle à l'aide d'un ensemble de traces publiques ainsi que des traces de trafic de notre base de données. La partie IV s'intéresse à l'utilisation de ce modèle pour du trafic contenant des anomalies et il est montré qu'il est alors possible de différencier un trafic avec anomalies d'un trafic sans anomalie et de classifier ces anomalies. Nous proposons alors une méthode de détection d'anomalie s'appuyant sur le modèle. Enfin, la partie V conclut cet article.

II Génération de traces de trafic avec et sans anomalies, par des expérimentations reproductibles

II.1 Besoin de traces d'expérimentations contrôlées et reproductibles

La pierre d'achoppement du travail d'analyse du trafic internet est souvent le manque de trace disponibles et une méconnaissance du trafic réellement présent, en particulier quand il vise à s'intéresser aux éventuelles anomalies. Les problèmes principaux des réseaux, notamment de qualité de service ou de sécurité, sont liés à des périodes au cours desquelles le trafic subit de fortes variations (particulièrement en volume). Pour pouvoir se focaliser sur ces périodes, il faut être capable à la fois de distinguer et de caractériser ce qu'est un trafic régulier et un trafic supposé anormal.

Un objectif du projet METROSEC est la détection d'anomalies par profil statistique. On s'intéresse principalement aux anomalies associées à des augmentations illégitimes du trafic, ou de certaines parties du trafic (paquets SYN, paquets ICMP, etc.). Nous visons à développer des outils de détection qui fonctionnent et restent efficaces même si l'augmentation de trafic est faible. Ce cas est fréquent et extrêmement important à cause de la nature distribuée des attaques de déni de service (*Distributed Denial of Service* – DDoS) actuelles. Ces attaques sont perpétrées depuis un grand nombre de machines corrompues (appelés zombies) et contrôlées par un pirate. Chaque machine génère une quantité infime de trafic d'attaque de façon à ce qu'il soit transparent à l'émission dans la masse du trafic Internet. Par contre, dès que ces nombreux trafics d'at-

taque s'agrègent sur les liens ou les routeurs menant à leur victime, ils représentent un volume considérable et diminuent significativement les performances de leur victime et du réseau auquel elle est connectée. La détection de l'anomalie est naturellement plus facile proche de la victime et une détection à ce stade est inutile : les ressources ciblées ont été gaspillées, la qualité du service dégradée ; l'attaque est un succès. Nous visons donc à détecter les attaques proches de leurs sources, lorsque l'anomalie n'est le résultat de l'agrégation des trafics que de quelques zombies, cachée dans la masse de trafics légitimes sur le réseau.

Il n'est pas aisé de se procurer des traces de trafic contenant ce genre d'anomalies. Il faudrait disposer de nombreuses sondes de capture de trafic en espérant en avoir certaines proches des zombies et enregistrer les traces au moment des attaques, supposant ensuite qu'on arrive à identifier a posteriori l'attaque. Evidemment les pirates ne préviennent pas lorsqu'ils lancent des attaques et les identités de leurs zombies sont inconnues. Nous ne disposons donc pas de traces de trafic documentées pour lesquelles aucune anomalie évidente n'apparaît, mais dont on saurait qu'entre telle et telle date une attaque d'un type référencé et d'une intensité précisée a été perpétrée. L'absence de telles traces est une difficulté pour la recherche sur les détections d'anomalies.[†] En outre, il n'est pas suffisant de valider les méthodes sur seulement une ou deux traces dans lesquelles des anomalies seraient identifiées par des outils ad-hoc, sans quantifier aussi les erreurs de détection. Il est nécessaire de disposer d'une large base de traces contenant des traces dans des conditions variées de trafic, à la fois de trafic normal et de situations contenant les différents types d'anomalies auxquelles on s'intéresse.

II.2 La plateforme expérimentale de METROSEC

Une des contributions de METROSEC est de produire des traces de trafic contrôlées et documentées pour tester et valider les modèles de trafic et les méthodes de détection d'intrusion. Ces traces sont utilisées ici pour la validation du modèle et de la méthode de détection que nous développons dans la suite.

Notre proposition a été de conduire des campagnes de mesure et d'expérimentations sur un réseau opérationnel fiable (pour lequel on est sûr qu'il ne contient pas d'anomalies ou peu) et de générer nous-mêmes des attaques ou d'autres d'anomalies qui vont passer par le réseau, se mélanger et interagir avec le trafic régulier. Il est ainsi possible de définir les types d'attaques que l'on souhaite perpétrer, de les contrôler (sources, cibles, intensités, etc.) et d'associer aux traces obtenues une documentation contenant les caractéristiques précises des anomalies. Dans un tel contexte, les anomalies sont reproductibles (on peut regénérer aussi souvent que l'on veut les mêmes conditions expérimentales) et on peut multiplier les réalisations pour augmenter les statistiques de validation des outils, ou comparer nos méthodes avec d'autres. C'est également le seul moyen de avoir des analyses robustes en vue de la caractérisation des trafics, car le trafic légitime est ici réel (et non modélisé ou simulé). La base de données de traces produites dans METROSEC est en soi un résultat du projet et garantit la fiabilité de l'évaluation du modèle.

La plate-forme expérimentale qui a servi à créer la base de traces de METROSEC utilise le réseau RENATER, le réseau national pour l'enseignement et la recherche (www.renater.fr). RENATER est un réseau opérationnel servant à une communauté nombreuse dans le cadre d'une activité professionnelle. Par sa conception, RENATER possède les qualités requises pour nos expérimentations :

- il est très largement sur-dimensionné par rapport au trafic qu'il transporte. Ses liens OC-48 offrent 2,4 Gbits/s de débit alors qu'un laboratoire comme le LAAS, disposant pourtant d'un lien d'accès de capacité 100 Mbits/s, génère en moyenne moins de 10 Mbits/s de trafic [38]. De fait, RENATER offre un service de qualité constante. Ainsi, même si nous souhaitions saturer le lien d'accès du LAAS, l'impact de RENATER sur ce trafic et la QoS fournie serait transparent. Les conditions expérimentales sur RENATER seront donc tout le temps équivalentes et par conséquent nos expérimentations reproductibles ;
- RENATER possède deux niveaux de sécurité pour éviter les attaques venant de l'extérieur mais aussi de l'intérieur du réseau. Pratiquement, nous n'avons effectivement jamais observé d'attaques au niveau des points de RENATER que nous supervisons.

Les sites impliqués dans la génération des traces sont l'ENS de Lyon, le LIP6 à Paris, l'IUT de Mont-de-Marsan, l'ESSI à Nice et le LAAS à Toulouse. Le trafic est capturé en ces différents points par des

[†] Ce manque est d'autant plus marqué par le fait que des raisons de stratégie économique des opérateurs ou de protection de la vie privée des utilisateurs contrarient en général la diffusion de données dans lesquelles des anomalies auraient été détectées.

stations équipées de cartes DAG [14] et de GPS pour une synchronisation temporelle de grande précision. De plus, lorsque l'on veut faire des attaques massives (ce qui reste rare vus les objectifs du projet), la cible est le réseau laasnetexp.fr du LAAS [30], qui est un réseau dédié aux expérimentations. Nous pouvons donc librement le saturer pour analyser les cas extrêmes d'attaques. Enfin, les chercheurs impliqués dans METROSEC ont accès à une plate-forme de machines aux capacités de stockage et de traitement importantes permettant l'analyse des traces collectées et classées dans la base de données.

II.3 Génération des anomalies

Les anomalies étudiées dans le cadre du projet METROSEC reposent sur des augmentations plus ou moins marquées en volume sur le trafic. On peut distinguer deux grands types d'anomalies :

- les anomalies provoquées par du trafic légitime. Citons par exemple les foules subites (*Flash Crowd* – FC). Il est à noter que le contrôle que nous pouvons avoir sur ces expérimentations est difficilement total ;
- les anomalies provoquées par du trafic illégitime, comme des attaques de flooding. Ce trafic, sur lequel nous avons un contrôle total, est issu de différents logiciels classiques d'attaque de DoS.

L'ensemble des traces issues des différentes campagnes de mesures est détaillé dans la section suivante II.4. Les mécanismes de génération des anomalies sont décrits ici.

• **Flash Crowd (FC) ou foule subite.** Pour analyser l'impact sur les caractéristiques du trafic d'un flooding dû à des variations légitimes du trafic, nous avons organisé des foules subites sur un serveur web. Pour les rendre réalistes, c'est-à-dire humainement aléatoires, nous avons choisi de ne pas les engendrer par un programme automatique, mais au contraire, de demander à nos collègues académiques de consulter le site web du LAAS (http ://www.laas.fr) à des dates décidées au préalable. Ceci garantit des traces représentatives d'un trafic intense dû à l'activité humaine, sans modèle.

• **Attaque DDoS.** Les attaques générées consistent principalement en des dénis de service distribués (DDoS), réalisés à l'aide de différents outils de flooding (IPERF, HPING2, TRIN00 et TFN2K). Nous avons privilégié l'utilisation de logiciels d'attaque bien connus, afin de générer des trafics malicieux les plus réalistes possibles.

Le logiciel IPERF [5] (sous environnement Linux standard) permet de générer des flux UDP à débits variables, en contrôlant le nombre de paquets émis par seconde et/ou la charge utile (payload) de chaque paquet. Le logiciel HPING2 [22] permet de générer des flux UDP, ICMP ou TCP à débits variables (avec les mêmes paramètres de contrôle du débit que pour IPERF). Notons que ce logiciel permet de plus de positionner les drapeaux TCP comme on le souhaite et donc de générer des signatures spécifiques dans les flux TCP. Nous avons installé ces deux logiciels sur chaque site de notre plateforme. Contrairement à TRIN00 et TFN2K (cf. ci-après), il n'est pas possible de centraliser la gestion des différentes instances de IPERF et HPING2, et donc de synchroniser les attaquants. Une personne sur chaque site doit lancer les attaques à un horaire prédéfini, ce qui induit, au niveau de la cible, une montée en charge progressive de l'attaque.

TRIN00 [48] et TFN2K [3] sont deux logiciels de dénis de service distribués bien connus. Ils permettent d'installer sur différentes machines un programme appelé zombie (ou démon, en anglais *bot*). Ce programme est chargé de générer l'attaque sur la cible. Il est contrôlé à distance par un programme maître, qui donne les ordres d'attaque aux différents bots. On constitue ainsi une véritable armée d'attaquants (*botnet*) commandés par un ou plusieurs maîtres.

Les bots TFN2K permettent de lancer plusieurs types d'attaques. Outre les flooding classiques utilisant les protocoles UDP, ICMP et TCP (envoi d'un grand nombre de paquets UDP, ICMP ou TCP SYN à la victime), d'autres attaques sont possibles. Le mixed flooding est un mélange de UDP flooding, ICMP flooding et TCP SYN flooding. Smurf est une technique d'attaque par amplification : les bots se servent d'adresses de broadcast pour multiplier artificiellement le nombre de paquets d'attaque destinés à la cible, et donc multiplier la puissance de cette attaque. Les bots TRIN00, quant à eux, ne peuvent faire que de l'UDP flooding.

Les attaques effectuées avec les différents logiciels d'attaque (IPERF, HPING2, TRIN00 et TFN2K) ont été réalisées en variant à dessein les caractéristiques et paramètres (durée, intensité du flux de déni

Logiciel	Type d'attaque	Durées traces			Durées attaques			Intensités		
Campagne de novembre-décembre 2004										
HPING	TCP flooding	1h23mn	1h23mn	3h3mn	15mn	13mn	3mn	30.77%	27.76%	90.26%
		3h3mn	3h3mn	30mn	7mn	8mn	5mn	70.78%	45.62%	91.63%
	UDP flooding	16h20mn (MetroSec-Ref1)			5mn			99.46%		
Campagne de juin 2005										
IPERF	UDP flooding	1h30	1h30	1h30	30mn	30mn	30mn	17.06% (I)	14.83%	21.51% (III)
		1h30	1h30	1h30	41mn	30mn	30mn	33.29%	39.26%	34.94%
		1h30	1h30	1h30	30mn	30mn	30mn	40.39%	36.93%	56.40%
		1h30			30mn			58.02% (G)		
Campagne de mars 2006										
TRINOO	UDP flooding	2h	1h	1h	10mn	10mn	10mn	7.0%	22.9%	86.8%
Campagnes d'avril à juillet 2006										
TFN2K	UDP flooding	2h	1h	30mn	11mn	10mn	10mn	92%	4.0%	7.0%
	ICMP flooding	1h30	1h		20mn	10mn		13%	9.8%	
	TCP SYN flooding	2h	1h		10mn	10mn		12%	33%	
	Mixed flooding	1h			10mn			27.3%		
	Smurf	1h			10mn			3.82%		

TAB. I: Description des attaques dans la base de traces. ***Description of the database of attacks.***

de service, taille et fréquence d'émission des paquets) afin de créer différents profils d'attaques. Les caractéristiques principales des attaques générées sont détaillées dans la table I. Chaque configuration a donné lieu à une capture de trafic avant, pendant et après les attaques, de façon à encadrer convenablement la période de DoS par deux périodes de trafic normal dans la même période d'utilisation du réseau (jour, horaire). Il est important de rappeler ici que la plupart du temps, nous avons généré des attaques de faible intensité de sorte qu'elles n'aient pas d'impact remarquable sur le trafic global (et par conséquent ne soient pas la cause de modifications de la moyenne du trafic). Cette situation émule le cas d'un routeur recevant les paquets venant d'un petit nombre de zombies et nous positionne donc dans le cas le plus intéressant de notre problématique, à savoir la détection d'attaques de DDoS proches de ses sources.

Notre base de traces comprend à ce jour une trentaine de captures d'expérimentations de ce type. C'est à partir de ces traces que nous validons le modèle proposé pour caractériser les trafics de l'Internet dans le cas de trafic avec anomalies. Ce modèle est justifié et présenté dans la partie III.

II.4 Description des traces servant d'exemples

• **Flash Crowd (FC) ou foule subite.** Les anomalies de foules subites que nous avons créées correspondent à un grand nombre d'utilisateurs humains qui viennent, sur une période courte et bornée, consulter le site web du LAAS. L'une de ces expérimentations est présenté en figure 1. Cette trace a été capturée pendant une expérience de foule subite réalisée le 14 avril 2005, qui a duré 30 minutes et a rassemblé plus de 100 participants. La figure 1(a) montre le nombre de requêtes reçues par le serveur web du LAAS (HTTP GET requests), en faisant la distinction entre les requêtes venant de l'intérieur et de l'extérieur du LAAS. Il apparaît clairement que de nombreux utilisateurs ont commencé à naviguer sur le site web du LAAS à 14h30 (augmentation importante du nombre de requêtes), mais également que la plupart ne sont pas restés pendant les 30 minutes. Les figures 1(b) et 1(c) montrent respectivement le nombre de flux et le débit des paquets sur le réseau d'accès du LAAS. Comme attendu, les deux courbes présentent une augmentation du nombre moyen de flux et du débit moyen de paquets, respectivement, durant la foule subite.

La figure 1(c) met aussi en évidence une augmentation du débit moyen (en paquets/s) avant l'expérience de foule subite. La figure 1(b) montre, quant à elle, une augmentation du nombre de connexions après l'expérience. Nous avons donc sur cette trace deux anomalies qui ne sont pas de notre fait et que nous devons donc analyser et expliquer.

Pour comprendre ces augmentations, nous avons analysé différentes composantes du trafic en utilisant l'outil *Traffic Designer* de la société QoSMOS [44] (cf. figure 1(d)). L'analyse a montré que l'anomalie autour de 14h (avant notre expérience) est due à des membres du LAAS qui naviguent sur le web juste après le déjeuner. Un tel comportement a été observé systématiquement sur toutes les traces collectées au LAAS depuis. Le second pic, après l'expérience, est dû à du trafic SMTP. Il peut s'expliquer de deux façons. En premier lieu, il faut savoir que de nombreux chercheurs au LAAS utilisent webmail. Comme le serveur a été très ralenti pendant l'expérience de foule subite (dégradation de la QoS), ils ont donc arrêté d'envoyer

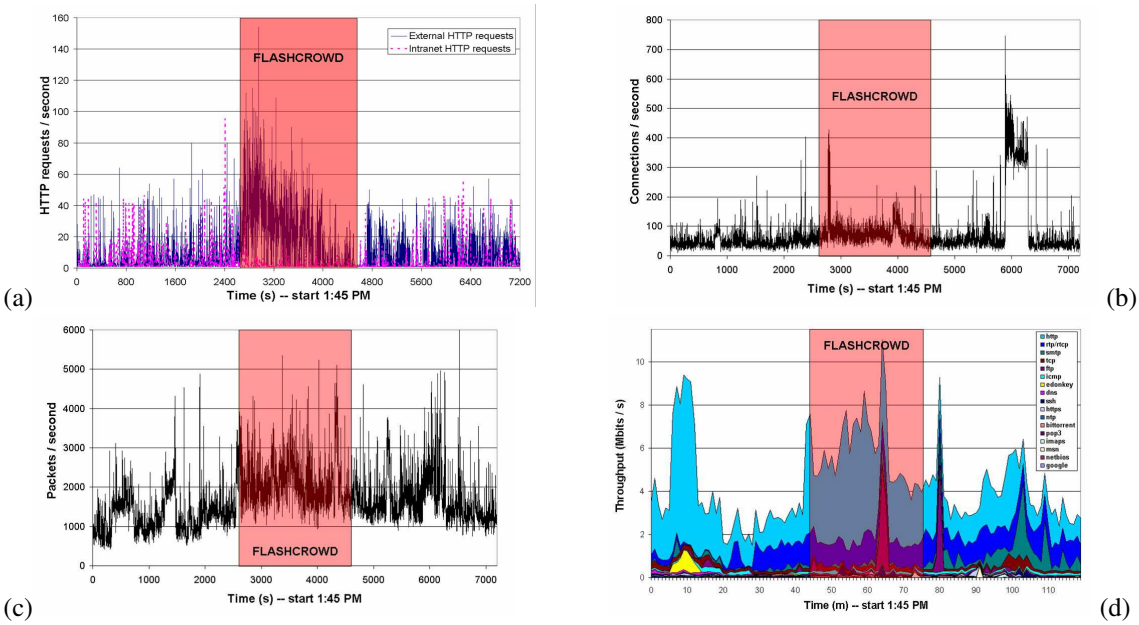

FIG. 1: Trace avec Flash Crowd. (a) Nombre de requêtes http, (b) de connexions, (c) de paquets par seconde et (d) distribution des débits par application (en Mbis/s). La figure (d) suit une approche descendante : l'application apparaissant en haut est celle qui génère le plus de trafic. ***Traffic with Flash Crowd.*** *(a) Number of http requests per second, (b) number of connections/s, (c) number of packets/s, (d) distribution of throughput per application (in Mbits/s). Figure (d) follows a top-down approach : application on the top is the one producing the most of traffic.*

des e-mails jusqu'à ce que le serveur recommence à fonctionner avec des performances satisfaisantes. Dans un second temps, il faut savoir que le mécanisme de *grey listing* (utilisé pour réduire le nombre de spam) retarde certains e-mails et les émet tous ensemble lors des ouvertures planifiées des portes. La première ouverture après l'expérience s'est produite à 15h15 et est la cause de l'augmentation de trafic constatée.

• **Attaques DDoS.** La figure 2 représente les débits en octets et paquets de trois expérimentations comportant des attaques, extraites de la campagne de juin 2005, que nous avons baptisées I, III et G. L'impact des attaques sur le débit global du lien analysé est variable, dépendant des paramètres choisis pour le flooding. Sur cette figure, on peut voir que deux attaques ont un impact important sur le profil du trafic global, tandis que la troisième attaque, au contraire, est totalement noyée dans le trafic global et donc quasiment invisible. Ceci est en accord avec l'objectif de détecter des attaques dont l'intensité reste faible et non complétement déployée. Les quelques attaques qui montrent une intensité forte nous servent à calibrer nos outils de détection.

III Modèle de processus non gaussien à mémoire longue

III.1 Choix du processus modélisant le trafic Internet

Les messages échangés par des ordinateurs sur un réseau peuvent être représentés par un processus d'arrivée de paquets. Il a été montré il y a plus de 10 ans qu'un modèle de Poisson n'est pas satisfaisant pour décrire ce processus (voir par exemple [41]), en particulier parce que les inter-arrivées de paquets ne sont pas indépendantes. Le processus d'arrivée des paquets a donc été représenté en utilisant soit des processus non stationnaires [28], soit des processus markoviens modulés stationnaires [4]. Une description générale de ce processus est $\{(t_l, A_l), l = 0, 1, 2, ...\}$, où t_l est l'estampille d'arrivée du l-ème paquet et A_l certains attributs du paquet (comme sa charge utile, ses ports source et destination,...). Cependant, le grand nombre de paquets impliqués rend difficile la manipulation de ces processus et des données nécessaires.

Une approche offrant plus de souplesse est de considérer les séries décomptant le nombre d'octets ou de paquets du trafic agrégé, notés $W_\Delta(k)$ et $X_\Delta(k)$. Elles correspondent au nombre d'octets (resp. paquets) qui transitent au cours de la k-ème fenêtre de taille $\Delta > 0$, i.e., dont les estampilles se situent entre $k\Delta \leq t_l <$

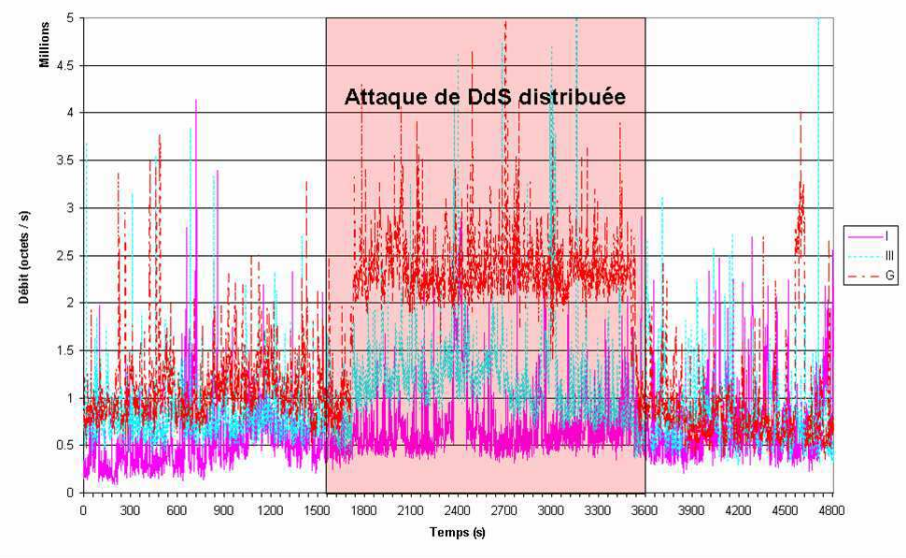

FIG. 2: Trafic collecté contenant des attaques de DoS (débit en octet/s). On montre ici 1h20 des traces contenant les attaques I, III et G (voir les caractéristiques dans la table I) pendant le second tiers-temps. ***Traffic with DoS attack (throughput in bits/s).*** *We show traces of duration 1h20, containing attacks I, III and G during the second third of the trace (see characteristics in table I).*

$(k+1)\Delta$. D'autres analyses reposent sur le processus d'arrivée des flux, comme par exemple dans [6]. Dans cet article, nous restons au niveau paquet, en nous concentrant sur la modélisation conjointe des distributions marginales et de la fonction de covariance du processus $X_\Delta(k)$. Modéliser la série temporelle $\{W_\Delta(k), k \in \mathbb{Z}\}$ donne des résultats équivalents mais, pour des raisons de clarté, nous nous limitons à la modélisation de la première série. Notons que nous n'utiliserons pas les propriétés statistiques d'ordre supérieur à 2. Les propriétés éventuelles de multifractalité (voir [19, 47, 54]) ne sont donc à prendre en compte ici.

III.2 Le modèle Gamma-farima

Le modèle proposé est un processus stationnaire, non gaussien et à longue mémoire : le processus Gamma (pour la loi marginale) - farima (pour la covariance covariance avec longue mémoire). Nous supposons que les séries à modéliser sont stationnaires pour simplifier les aspects théoriques. Dans la suite, nous vérifions empiriquement la validité de cette propriété durant les analyses de traces.

• **Statistiques du premier ordre (lois marginales) : distributions Gamma.** $X_\Delta(k)$ est par définition une variable aléatoire positive. Des travaux ont proposé de décrire sa loi marginale avec des lois positives bien connues comme les lois exponentielle, log-normale, Weibull ou des distributions Gamma [35]. Par nature $X_\Delta(k)$ est l'agrégation d'un processus d'arrivées de paquets et on peut s'attendre à des distributions Poisson ou exponentielle pour les niveaux de faible agrégation Δ. Pour des données fortement agrégées, les lois gaussiennes constituent de bonnes approximations. Cependant, aucune de ces lois ne peut modéliser de façon satisfaisante les lois marginales du trafic pour un spectre large de (petits et grands) Δ. Nos études empiriques montrent que la famille des distributions Gamma $\Gamma_{\alpha,\beta}$ s'ajuste au mieux aux marginales de X_Δ à toutes les échelles de temps d'agrégation.

Une distribution $\Gamma_{\alpha,\beta}$ est définie pour des variables aléatoires positives X par

$$\Gamma_{\alpha,\beta}(x) = \frac{1}{\beta}\Gamma(\alpha)\left(\frac{x}{\beta}\right)^{\alpha-1}\exp\left(-\frac{x}{\beta}\right), \tag{1}$$

où $\Gamma(u)$ est la fonction Gamma standard (voir [17]). Elle dépend de deux paramètres : la forme α et l'échelle β. Sa moyenne est $\mu = \alpha\beta$ et sa variance $\sigma^2 = \alpha\beta^2$. À noter que l'inverse du paramètre de forme, $1/\alpha$, agit comme un indicateur de la distance avec une loi gaussienne.

• **Statistiques du second ordre (covariance) : dépendance à long terme.** Depuis les travaux présentés dans [32], il est accepté que le trafic sur un réseau d'ordinateurs présente des propriétés de mémoire longue ou de dépendance à long terme [9]. La dépendance à long terme (ou *Long Range Dependence*, soit LRD) est définie par le comportement à l'origine de la densité spectrale en puissance du processus, notée $f_{X_\Delta}(\nu)$:

$$f_{X_\Delta}(\nu) \sim C|\nu|^{-2d},\ |\nu| \to 0,\ \text{ avec } 0 < d < 0.5. \tag{2}$$

Cette longue mémoire est une caractéristique importante du trafic Internet qui entraîne des baisses de performance et de QoS [20]. Dans la conception des réseaux (adaptation aux besoins de la taille des buffers, dimensionnement,...) et dans l'étude de leurs performances, il est crucial d'incorporer la LRD. De ce fait, les processus poissonniens ou markoviens, ainsi que leurs déclinaisons, sont difficilement employables pour ces tâches.

Il faut par conséquent se tourner vers les modèles directement construits avec une longue mémoire comme les mouvement browniens fractionnaires, les bruits gaussiens fractionnaires [37] ou les modèles *Fractionally Integrated Auto-Regressive Moving Average* (farima) [9]. Ces modèles ont été largement utilisés pour décrire et analyser les séries temporelles extraites du trafic Internet (voir [40] et les références associées). La multitude de mécanismes réseaux (allers-retours rapides de paquets) et de sources de trafic différents font que des dépendances à court terme se superposent à celles de mémoire longue. Il est intéressant de les modéliser aussi, tel que cela a été étudié par exemple pour le trafic vidéo VBR [23]. Les processus farima [9] sont alors des modèles naturels pouvant décrire à la fois la mémoire longue et les corrélations à court terme. Un modèle farima(P,d,Q) est défini par sa densité spectrale de puissance. Le coefficient $d \in [-1/2, 1/2]$ est associé à une intégration fractionnaire et deux polynômes d'ordre P et Q ajustent les corrélations à temps courts de telle sorte que :

$$f_X(\nu) = \sigma_\varepsilon^2 |1 - e^{-i2\pi\nu}|^{-2d} \frac{|1 - \sum_{q=1}^{Q} \theta_q e^{-iq2\pi\nu}|^2}{|1 - \sum_{p=1}^{P} \phi_p e^{-ip2\pi\nu}|^2}, \tag{3}$$

pour les fréquences $-1/2 < \nu < 1/2$. Une conséquence immédiate est que, pour $d \in (0, 1/2)$, ce processus est à mémoire longue. Les polynômes d'ordre P et Q permettent de reproduire le spectre aux hautes fréquences (i.e. les petites échelles), alors que d représente l'intensité de la mémoire longue (i.e. les grandes échelles).

Pour les analyses et exemples présentés dans cet article, il est suffisant de recourir à des polynômes P et Q de degrés au plus égal à 1, de coefficient respectivement ϕ et θ. Les processus $\Gamma_{\alpha,\beta}$-farima(ϕ, d, θ) comportent ainsi 5 paramètres qu'il faut extraire des données. Ils forment une famille de modèles simples ce qui est une propriété importante si on veut pouvoir l'utiliser pour une analyse à la volée (ou en temps-réel) du trafic qui soit robuste et efficace. Il faut toutefois noter que les premier et second ordres statistiques ne caractérisent pas complètement le processus car il est non gaussien. Il reste donc une marge d'amélioration du modèle pour qu'il décrive plus finement les autres propriétés du trafic. Toutefois, cette tâche n'est pas nécessaire pour les caractéristiques du trafic que nous souhaitons pouvoir décrire dans cet article.

III.3 Analyse du modèle Gamma-farima

On peut modéliser X_Δ pour chaque niveau d'agrégation. Étant donné l'hypothèse de stationnarité de X_Δ dont nous avons besoin pour la modélisation théorique, nous commençons par une vérification empirique des analyses et estimations obtenues sur des sous-blocs adjacents et disjoints. Ensuite, nous analysons seulement les ensembles de données pour lesquels la stationnarité est une hypothèse raisonnable. C'est une approche dont l'esprit est très proche de celle développée dans [51]. Sur chaque période de temps où le trafic est stationnaire, nous mettons en œuvre la procédure suivante d'estimation des paramètres du modèle pour chacun des Δ choisis.

• **Estimation des paramètres de la loi Gamma.** Les paramètres peuvent être obtenues via les deux premiers moments $\beta = \sigma^2/\mu$, $\alpha = \mu/\beta$ où μ et σ^2 sont les estimateurs standard pour la moyenne et la variance. Nous utilisons plutôt ici pour une plus grande robustesse la technique du maximum de vraisemblance [21]. Cependant il faut noter que le terme « maximum de vraisemblance » est ici utilisé abusivement

Données	Date(Date de début)	T (s)	Réseau(Lien)	# Pkts	IAT (ms)	Répertoire
PAUG	1989-08-29(11 :25)	2620	LAN(10BaseT)	1	2.6	ita.ee.lbl.gov
LBL-TCP-3	1994-01-20(14 :10)	7200	WAN(10BaseT)	1.7	4	ita.ee.lbl.gov
AUCK-IV	2001-04-02(13 :00)	10800	WAN(OC3)	9	1.2	wand.cs.waikato.ac.nz
CAIDA	2002-08-14(10 :00)	600	Backbone(OC48)	65	0.01	www.caida.org
UNC	2003-04-06(16 :00)	3600	WAN(10BaseT)	4.6	0.8	www-dirt.cs.unc.edu
METROSEC-ref1	2004-12-09(18 :30)	5000	LAN(10BaseT)	3.9	1.5	www.laas.fr/METROSEC/

TAB. II: Description des données publiques employées. T est la durée de la trace, en secondes. # Pkts (10^6) est le nombre de paquets dans la trace, en millions. IAT est le temps d'inter-arrivées moyen, en ms. **Description of the public traces which were used.** *T is the duration in seconds. # Pkts (10^6) is the number of packets in the trace, in millions. IAT is the mean inter-arrival time between packets, in ms.*

car, dans notre cas, les $X_\Delta(k)$ ne sont pas indépendants. Il a été vérifié empiriquement à partir de simulations numériques que cette procédure d'estimation donne des résultats très précis, même lorsqu'elle est appliquée à des processus à longue mémoire [45].

• **Estimation des paramètres du farima.** L'estimation du paramètre de mémoire longue est une question difficile déjà largement étudiée (voir [15] par exemple). L'estimation conjointe des paramètres de mémoire courte et longue du processus farima(ϕ, d, θ) est en théorie possible par une méthode d'estimation basée sur le maximum de vraisemblance fondée sur la forme analytique du spectre (équation 3). Cependant une telle approche est lourde en temps de traitement.

En remplacement, nous avons donc développé une procédure d'estimation en deux étapes : tout d'abord, nous estimons le paramètre de LRD d en utilisant une méthode basée sur une décomposition en ondelettes. Cette méthode n'est pas détaillée dans cet article. Le lecteur pourra se référer à [2, 50]. Elle consiste en l'estimation du paramètre d à partir de la pente à grande échelle dans le diagramme log-échelle qui représente le logarithme du spectre en ondelettes en fonction du logarithme de l'échelle. Ensuite, à partir de cette estimation de d, nous opérons une dérivation fractionnaire d'ordre d de X_Δ. On élimine ainsi la LRD du processus de sorte qu'il ne reste plus que les composants ARMA (estimation des corrélations à temps courts). Une procédure itérative classique (basée sur l'algorithme de Gauss-Newton) [34] est alors employée pour estimer les paramètres ARMA. La principale faiblesse de cette procédure d'estimation en deux phases se situe au niveau de la qualité de l'estimation de d. Si d est mal estimé, les paramètres ARMA le seront aussi. La qualité des estimations obtenues avec cette procédure a été étudiée numériquement dans [45] à partir de processus $\Gamma_{\alpha,\beta}$-farima(ϕ, d, θ) synthétisés numériquement. Les résultats obtenus ont validé cette méthode d'estimation.

III.4 Trafic sans anomalie

Ces procédures d'estimation ont été appliquées aux séries temporelles du trafic, indépendamment pour différents niveaux d'agrégation. Nous présentons ici les résultats détaillés pour les séries issues des traces **AUCK-IV** et **MetroSec-ref1**. Des résultats similaires ont été obtenus pour les autres traces citées dans les tableaux I et II, mais nous ne les présentons pas dans cet article par manque de place.

• **Marginales.** Les figures 3 et 5 illustrent l'adéquation des distributions marginales des processus $\Gamma_{\alpha,\beta}$ avec X_Δ pour un large spectre de niveaux d'agrégation : 1ms $\leq \Delta \leq$ 10 s, respectivement pour les deux trafics d'illustration. Cette adéquation a été caractérisée au moyen de tests de χ^2 et de Kolmogorov-Smirnov (non décrits dans l'article). Notons que les distributions Gamma démontrent en général une meilleure adéquation aux données que celle obtenue avec des lois exponentielles, log-normales ou de χ^2. Pour certaines des séries analysées et certains niveaux d'agrégation, l'une ou l'autre de ces lois peut approximer plus précisément les données que la loi Gamma. Toutefois, les distributions Gamma ne sont jamais très éloignées des données réelles et même si une distribution particulière approxime mieux les données que la loi Gamma pour un Δ donné, cela n'est pas le cas sur un tout un ensemble de valeurs Δ. À l'opposé, l'adéquation des lois Gamma reste très satisfaisante pour un large spectre de valeurs de Δ et révèle que la caractérisation des marginales du trafic dépend fortement de l'échelle d'observation. Les lois $\Gamma_{\alpha,\beta}$ adaptent l'évolution de leurs paramètres de formes et d'échelles et offrent une évolution continue et stable d'une loi exponentielle pure vers une loi gaussienne.

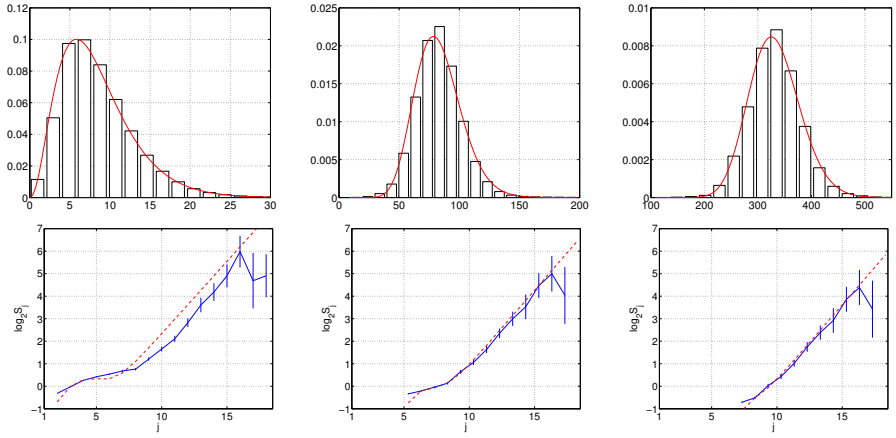

FIG. 3: AUCK-IV. Ajustement des marginales (en haut) et des covariances (en bas) empiriques par celles du processus $\Gamma_{\alpha,\beta}$-farima(ϕ,d,θ) pour $\Delta = 10, 100, 400$ ms (de gauche à droite) ; $j = 1$ correspond à 10 ms. **AUCK-IV.** *Fits of the empirical marginal PDFs (up) and covariances (bottom) of the* $\Gamma_{\alpha,\beta}$*-farima*(ϕ,d,θ) *process for* $\Delta = 10, 100, 400$ *ms (from left to right) ;* $j = 1$ *corresponds to 10 ms.*

Ensemble, ces observations militent en faveur de l'utilisation de lois Gamma pour modéliser les marginales du trafic internet. Un autre argument est que les lois Gamma forment une famille qui reste stable par l'opération d'addition : pour des variables aléatoires indépendantes X_i (avec $i = 1,2$), de lois $\Gamma_{\alpha,\beta}$, leur somme $X = X_1 + X_2$ suit une loi $\Gamma_{\alpha_1+\alpha_2,\beta}$. L'agrégation de données correspond à $X_{2\Delta}(k) = X_\Delta(2k) + X_\Delta(2k+1)$. En utilisant la propriété de stabilité par addition et sous hypothèse d'indépendance des lois, α devrait augmenter de façon linéaire avec Δ alors que β reste constant. La première ligne (haute) des figures 4 et 6, montre l'évolution de α et β en fonction de $\log_2 \Delta$. Pour toutes les séries temporelles, des écarts significatifs par rapport à ces comportements sous hypothèse d'indépendance sont observés. Une analyse attentive montre que $\alpha(\Delta)$ n'augmente pas pour les petites valeurs de Δ, puis augmente quasiment comme $\log_2 \Delta$ pour des valeurs de Δ plus grandes, alors que le comportement de $\beta(\Delta)$ est proche d'une augmentation en loi de puissance. C'est une signature de l'existence de corrélations à courts temps (puisque, comme nous le discuterons plus loin $\Delta \simeq 1$ s est dans la zone de domination de la longue mémoire dans le trafic). Les variations conjointes de α et β en fonction du niveau d'agrégation Δ sont utilisables comme propriétés caractéristiques du trafic normal. Nous allons dans la suite utiliser cette propriété pour caractériser et classifier le trafic avec anomalies.

• **Covariances.** Pour les deux séries de référence, la ligne du bas des figures 3 et 5, compare les diagrammes log-échelle des spectres en ondelettes obtenus à partir des données avec ceux obtenus avec le modèle. Ces courbes illustrent l'adéquation des covariances du processus farima(ϕ,d,θ) et de X_Δ. Lorsque Δ augmente, on peut remarquer que les diagrammes log-échelle sont quasiment identiques à ceux obtenus pour des Δ plus petits, en les tronquant aux échelles plus grandes. Ceci s'explique par le fait que l'agrégation de données consiste à lisser les détails qui apparaissent à des petites échelles, mais qui n'affectent en rien les grandes échelles. L'agrégation n'élimine donc, ni n'altère la caractéristique de longue mémoire. Ceci se vérifie sur les figures 4 et 6 (en bas à gauche), où l'on voit que d reste pour l'essentiel indépendant de Δ. Ceci, une nouvelle fois, souligne que la LRD capture un attribut de longue durée sur le trafic qui n'apparaît pas pour des échelles intermédiaires.

D'un autre côté, les corrélations à courts termes sont éliminées lorsque le niveau d'agrégation augmente. On peut voir sur ces mêmes figures en bas à droite, que ϕ et θ baissent de façon significative lorsque Δ augmente. Ils devraient se rejoindre et se compenser si le niveau d'agrégation Δ devient plus grand que les échelles caractéristiques des corrélations à temps courts. La covariance converge théoriquement vers celle d'un bruit gaussien fractionnaire qui s'avère, pratiquement, être extrêmement proche de celle d'un processus farima$(0,d,0)$. Pour toutes les séries temporelles de référence étudiées ici, l'échelle temporelle pour laquelle la mémoire longue est dominante (mesurée comme le niveau d'agrégation approximatif Δ

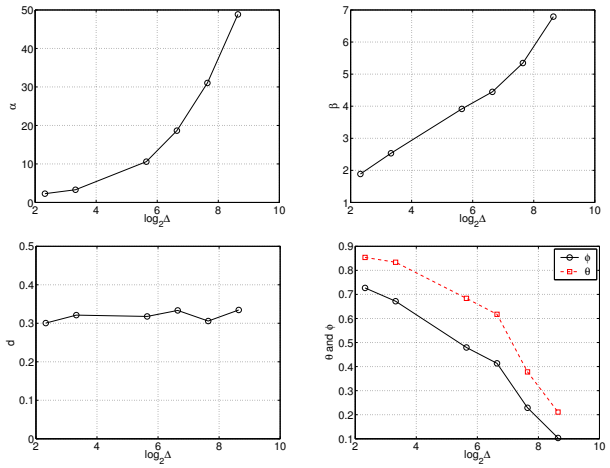

FIG. 4: AUCK-IV. Paramètres estimés du processus $\Gamma_{\alpha,\beta}$-farima(ϕ,d,θ) en fonction de $\log_2\Delta$ (avec Δ en ms). **AUCK-IV.** *Estimation of the parameters of the* $\Gamma_{\alpha,\beta}$*-farima*(ϕ,d,θ) *process, as functions of* $\log_2\Delta$ *(*Δ *is in ms).*

pour lequel la partie ARMA du modèle disparaît) correspond à $\Delta \geq 600$ ms .

• **Conclusions.** Nous avons mis l'accent sur le fait que pour un large ensemble de traces de trafic collectés dans des conditions et sur des réseaux différents, le modèle $\Gamma_{\alpha,\beta}$-farima(ϕ,d,θ) proposé reproduit précisément les marginales ainsi que les corrélations à court et long terme des séries temporelles. Le fait que le modèle proposé est suffisamment versatile pour travailler efficacement à différents niveaux d'agrégation est un élément clef pour deux raisons :

1. un problème récurrent de la modélisation du trafic concerne le choix d'un niveau d'agrégation Δ pertinent. C'est une question délicate dont la réponse devrait tenir compte des caractéristiques des données, de l'objectif de la modélisation, ainsi que de problèmes techniques comme les contraintes de temps réel, de taille des tampons ou de coût de traitement. Par conséquent, choisir Δ a priori peut être très difficile. L'utilisation d'un processus qui offre une modélisation évolutive en fonction de Δ permet de contourner cette question ;
2. les valeurs des paramètres du modèle varient, souvent de façon importante d'une situation à l'autre. Mais ce ne sont pas les valeurs elles-mêmes qui sont importantes, en particulier pour caractériser le trafic (ou détecter des anomalies), mais les courbes d'évolution de ces paramètres en fonction de Δ qui offrent des éléments statistiques pertinents d'analyse du trafic internet.

IV Trafic avec anomalies : modélisation et détection

IV.1 Analyse et détection d'anomalies

L'enjeu de la modélisation de trafic est de construire des systèmes de détection d'intrusions (IDS) qui réagissent aux comportements anormaux de trafic. Les IDS visant la détection d'anomalies n'utilisent pas, en général, des modèles statistiques riches. Ils supervisent des paramètres simples du trafic comme son débit d'octets ou de paquets, ou recherchent des séquences de paquets spécifiques, connues comme des signatures d'attaques [42]. Les alarmes sont alors générées lorsqu'un seuil est dépassé [49], ce qui conduit à un nombre important de faux positifs [36]. Par conséquent, ces IDS sont souvent assez peu satisfaisants car ils ne savent pas différencier les variations légitimes du trafic et les attaques. Certains travaux cherchent cependant à mieux analyser le trafic au niveau des applications [18] ou les mécanismes des attaques [27], ou encore à discriminer au niveau des requêtes web entre les attaques et les variations légitimes de trafic, parfois très importantes [26].

Une autre approche est de travailler au niveau des paquets en s'appuyant sur les progrès récents en modélisation de trafic, obtenus dans les projets de métrologie. Ils ont renouvelé les stratégies de conception des nouveaux IDS [12] et des résultats intéressants utilisant des caractérisations statistiques ont été publiés.

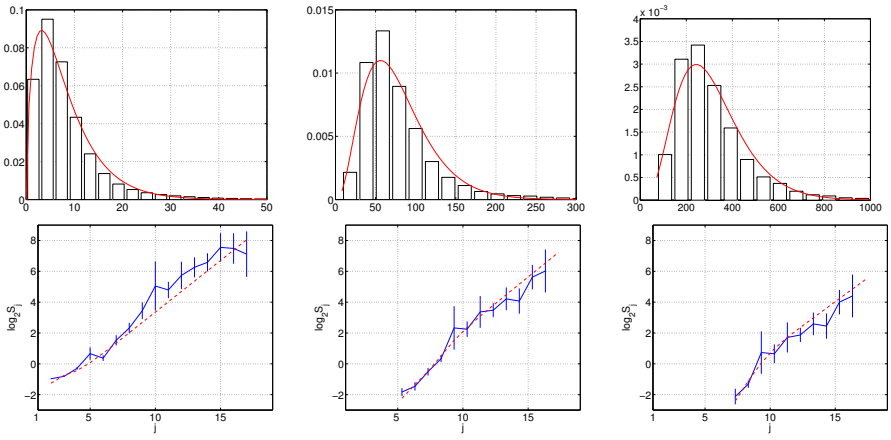

FIG. 5: Metrosec-ref1. Ajustement des marginales (en haut) et des covariances (en bas) empiriques par celles du processus $\Gamma_{\alpha,\beta}$-farima(ϕ,d,θ) pour $\Delta = 10,100,400$ ms (de gauche à droite en bas). $j = 1$ correspond à 10 ms. **Metrosec-ref1.** *Fits of the empirical marginal PDFs (up) and covariances (bottom) of the $\Gamma_{\alpha,\beta}$-farima(ϕ,d,θ) process for $\Delta = 10,100,400$ ms (from left to right) ; $j = 1$ corresponds to 10 ms.*

Par exemple, Ye propose dans [52] un modèle markovien pour le comportement temporel du trafic qui génère des alarmes lorsque le trafic s'éloigne significativement du modèle. D'autres auteurs [25, 53] ont montré que les attaques de DoS augmentent la corrélation dans le trafic, ce qui ouvre la voie vers des techniques de détection robuste. Partant de l'évaluation de l'inter-corrélation de trafics sur différents liens, Lakhina *et al.* ont proposé une méthode pour détecter les anomalies dans les matrices de trafic à l'échelle du réseau global [31]. Hussain et ses co-auteurs utilisent la densité spectrale pour identifier des signatures pour différentes attaques [24]. De la même façon, l'estimation spectrale a été utilisée pour comparer des trafics avec et sans attaques [13]. Alors que la densité spectrale met en évidence des pics autour du RTT pour du trafic normal, ces pics disparaissent en cas d'attaque. Cette caractéristique peut ainsi être utilisée pour concevoir de nouveaux IDS. Enfin, Li and Lee ont utilisé les techniques à base d'ondelettes développées dans [50] pour calculer une distribution d'énergies. Ils ont observé que cette distribution d'énergie présente des pics lorsque le trafic contient des attaques qui n'existent pas pour le trafic régulier [33]. Le travail présenté dans [7] exploite les qualités d'analyse multi-résolutions des décompositions en ondelettes pour détecter les anomalies du trafic pour un intervalle d'échelles moyennes.

Dans ce travail, nous nous focalisons sur les anomalies au niveau paquet IP. Nous montrons dans la suite que le modèle non gaussien multirésolution reste valide pour décrire les statistiques de trafic en présence d'anomalies. Ceci est montré sur des traces de la base de donnée METROSEC, à la fois pour les anomalies de DDoS et celles de Flash Crowds. En comparant alors les distributions marginales et les fonctions de covariance entre des situations de trafic régulier et des cas de trafic avec anomalies, nous construisons une méthode à même de détecter les changements de trafic dus à des actions illégitimes, tout en les discriminant de ceux dus à des actions légitimes.

IV.2 Modélisation du trafic en présence d'attaques de DDoS

Nous montrons d'abord que le modèle s'ajuste pour décrire convenablement le trafic agrégé quand une attaque de DDoS existe, mais avec des paramètres aux caractéristiques spécifiques [10]. La covariance, estimée via les diagrammes log-échelles, est présentée sur la figure 7, et les lois marginales sont montrées en figure 8 (courbes de gauche). Sont représentés sur la première figure, les diagrammes log-échelles estimés pendant des périodes de trafic régulier, avant et après l'attaque de DoS. Les estimations sont faites sur une demi-heure de trafic dans chaque situation. Ces courbes montrent que le modèle Γ-farima(ϕ,d,θ) décrit de façon satisfaisante le trafic contenant une attaque DDoS.

Pour des échelles supérieures à 500 ms ($j = 9$ sur la figure 7), aucune différence n'est visible entre la période d'attaque et celles avant ou après l'attaque. Le paramètre de LRD, d, reste en particulier constant.

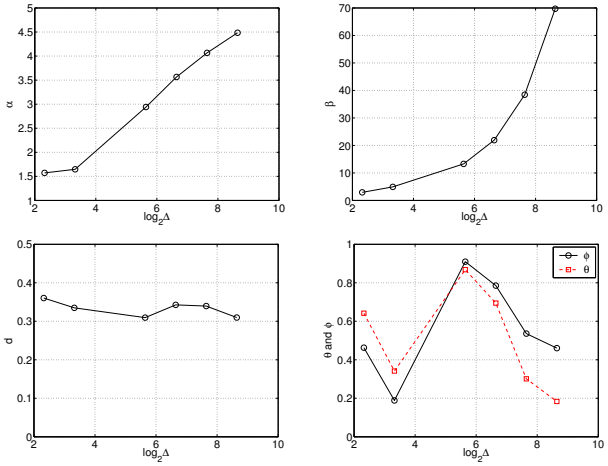

FIG. 6: Metrosec-ref1. Paramètres estimés du processus $\Gamma_{\alpha,\beta}$-farima(ϕ,d,θ), en fonction de $\log_2\Delta$ (Δ en ms). **Metrosec-ref1.** *Estimation of the parameters of the* $\Gamma_{\alpha,\beta}$*-farima*(ϕ,d,θ) *process, as functions of* $\log_2\Delta$ *(*Δ *is in ms).*

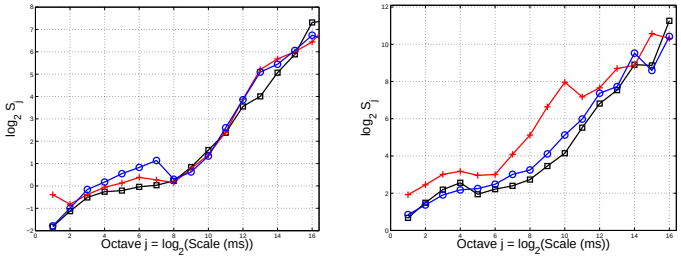

FIG. 7: Diagrammes log-échelle. Attaque DDoS (à gauche) et Flash Crowd (à droite). $\Delta = 1$ ms correspond à $j = 0$. Pour les deux événements, les courbes sont données pour la période de l'anomalie (croix sur la courbe), avant l'anomalie (carrés) et après (cercles), ces deux derniers cas constituant des références de trafic normal. ***Log-scale Diagrams.*** *DDoS attack (left) and Flash Crowd (right).* $\Delta = 1$ *ms corresponds to* $j = 0$*. For both anomalies, the curves are given during (crosses), before (squares) and after (circles) the anomaly, the last two cases being regular traffic.*

Cela signifie que la LRD n'est pas créée par l'attaque et également qu'elle lui est insensible. La seule différence sur le diagramme log-échelle est une augmentation relative pour les échelles $j = 4$ à 7 après l'attaque : cela est dû au fait que les séries du trafic après l'attaque ont été capturées la nuit, avec donc une charge relative plus faible du trafic liés à des longues sessions (partie du diagramme log-échelle à des échelles plus grandes que 1 s). Une première conclusion est donc que l'anomalie ne peut pas être décelée comme un changement de comportement de la longue mémoire.

Les courbes de la figure 9 comparent les évolutions des estimations des paramètres α et β en fonction de Δ pour du trafic pendant (croix), avant (carrés) et après (cercles) l'attaque DDoS. Les fonctions $\alpha(\Delta)$ et $\beta(\Delta)$ pendant l'attaque s'écartent significativement des comportements réguliers, le changement se traduisant par une forme des courbes (en fonction de Δ) qui n'est plus la même. Insistons sur un point : en situation de trafic normal les valeurs des paramètres peuvent varier d'un bloc à l'autre mais les évolutions en fonction de Δ restent comparables entre elles, alors que les trafics anormaux entrainent un schéma d'évolution différent à travers les échelles. L'attaque produit une augmentation immédiate et brutale de α dès les petites valeurs de Δ alors que dans des conditions normales α reste constant ou ne présente que des variations limitées, et ce pour $\Delta \simeq 20$ ms. L'évolution de β est à l'opposé : il reste petit de $\Delta \simeq 1$ ms à $\Delta \simeq 30$ ms pendant l'attaque DDoS, alors qu'il augmente régulièrement avec Δ dans des conditions normales de trafic.

Ces évolutions s'interprètent en termes d'occurrence de l'événement « recevoir 0 paquet pendant Δ » et d'un effet de « gaussianisation ». Premièrement, comme pendant l'attaque un grand nombre de paquets est émis avec un débit le plus élevé possible, une caractéristique de la trace est la possibilité pour un observateur de ne voir aucun paquet (événement « 0 paquet ») dans une fenêtre de taille Δ qui diminue très

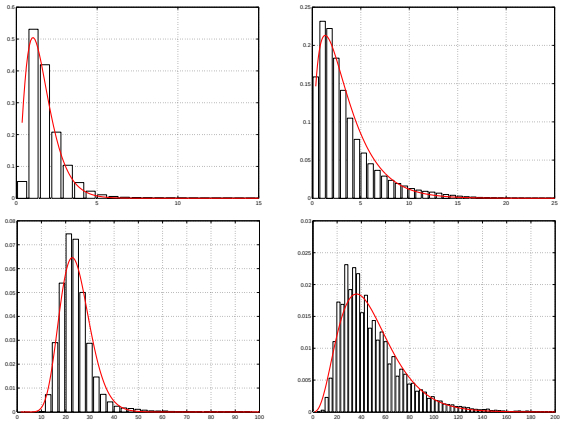

FIG. 8: Lois marginales. Attaque DDoS (à gauche) et Flash Crowd (à droite). On représente les histogrammes empiriques de X_Δ, en adéquation avec les marginales modélisées par des lois $\Gamma_{\alpha,\beta}$ pour $\Delta = 2$ms (haut) et $\Delta = 32$ms (bas). ***Marginal PDFs.*** *DDoS attack (left) and Flash Crowd (right). We show the empirical histograms of X_Δ, fitted with the marginal probability density functions as modeled by $\Gamma_{\alpha,\beta}$ laws, for $\Delta = 2ms$ (top) and $\Delta = 32ms$ (bottom).*

vite jusqu'à 0 dès que Δ atteint 1 ms. Plus précisément, on observe que la probabilité marginale lors d'une attaque DDoS d'avoir un très petit nombre de paquet (zéro en particulier) est nulle en-deça d'un seuil qui dépend du temps d'observation Δ. C'est différent de ce qui se passe en trafic régulier où les distributions décroissent lentement vers 0 lorsque $X_\Delta \to 0$ (comparer les figures 3 ou 5 avec la figure 8). Cet effet a précisément un impact sur les valeurs prises par le paramètre de forme α en fonction de Δ, impliquant que α croît lentement avec Δ pour le trafic régulier et beaucoup plus rapidement pour celui qui contient une attaque. Deuxièmement, comme c'est mentionné dans la partie III.2 plus haut, $1/\alpha$ contrôle l'écart entre les distributions $\Gamma_{\alpha,\beta}$ et gaussiennes. Ce paramètre α tend à toujours croître avec le niveau d'agrégation. Toutefois, les attaques DDoS accélèrent cette croissance avec l'effet de « gaussianisation ». Ceci constitue une particularité statistique qui différencie le trafic contenant des attaques du trafic régulier. Pour finir, il faut noter que cet effet implique des échelles pour le trafic allant de 1 ms à $0,5$ s mais que la partie ARMA du modèle de covariance ne capture que difficilement ce changement de corrélation.

IV.3 Procédure de détection de DDoS.

Comme application de la procédure de modélisation du trafic, nous proposons une stratégie de détection des attaques par DDoS adaptant simplement les méthodes de détection statistique à la situation présente. Elle consiste à analyser le trafic sur des fenêtres successives disjointes de durée T. Les paramètres de la modélisation sont estimés pour chaque fenêtre, en notant l l'index de temps ($l \in \mathbb{Z}$). On calcule alors une distance entre ces paramètres et ceux estimées lors du trafic en situation normale. L'étape de détection revient à décider qu'on est en présence de trafic anormal quand la distance devient suffisamment grande. Une telle méthode laisse trois choix à faire a priori : choisir la situation de référence pour définir les paramètres de trafic normal, choisir le type de distance à employer et enfin fixer un seuil d'alarme.

• **Choix de la distance.** Il existe une grande variété de distances pertinentes (voir [8] pour une revue exhaustive). Nous proposons ici de regarder comment se comportent deux choix simples, qui vont se révéler être des métriques de détection efficaces. La première est une distance quadratique moyenne prise dans l'espace des paramètres α et β multirésolution :

$$D_\alpha(l) = \frac{1}{J}\sum_{j=1}^{J} \left(\alpha(\Delta_j)_l - \alpha(\Delta_j)_{ref}\right)^2, \quad D_\beta(l) = \frac{1}{J}\sum_{j=1}^{J} \left(\beta(\Delta_j)_l - \beta(\Delta_j)_{ref}\right)^2 \tag{4}$$

Ces distances, quoique simples, ont pour intérêt majeur de combiner les propriétés du modèle à différents niveaux d'agrégation $\Delta_j = \Delta_0 2^j$ (où $\Delta_0 = 1$ ms). L'autre distance est de type informationnelle : la divergence

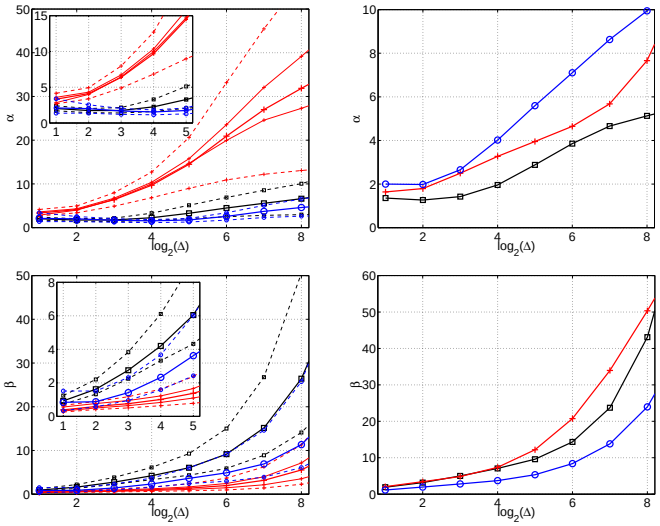

FIG. 9: Estimation des paramètres $\Gamma_{\alpha,\beta}$. Estimation de α (haut) et β (bas) en fonction de $\log_2 \Delta = j$ (Δ en ms) pour l'attaque DDoS (gauche) et pour la Flash Crowd (droite). Dans les deux cas, les courbes sont données pour les périodes de l'anomalie (croix), avant (carrés) et après (cercles). Pour l'attaque **DDoS**, l'évolution moyenne des paramètres (ligne épaisse) est dessinée et superposée avec les valeurs extrêmes prises pendant chaque période (lignes pointillées). Dans l'exemple, deux évolutions typiques pendant l'attaque sont présentées sur le graphe (lignes fines). Un zoom sur les petites échelles est ajouté en encart. Pour la **FC** on montre l'estimation des paramètres pendant l'anomalie et pour le trafic de référence (avant et après la FC). ***Estimated*** $\Gamma_{\alpha,\beta}$ ***parameters.*** *Estimation of* α *(top) and* β *(bottom) as a function of* $\log_2 \Delta$ *(*Δ *in ms) for the DDoS Attack (left) and for the Flash Crowd (right). In both cases, the curves are given during (crosses) before (squares) or after (circles) the anomaly. For the* ***DDoS****, the mean evolution (thick line) of the parameters on various 15 min data blocks is drawn, superimposed with the extremal values taken during each period (dashed lines) ; for the sake of example, two typical evolutions over one block during the DDoS are shown (in thin lines) on the graph. A zoom for the small scales is shown as an inside-plot. For the* ***FC*** *event estimation on a 15 min. window is reported for each period (before, during and after the event).*

de Kullback-Leibler entre les lois de probabilités f au temps de mesure et celles de référence.

$$KD(f_l, f_{ref}) = \int (f_1 - f_{ref})(\ln f_l - \ln f_{ref})dx. \tag{5}$$

Elle peut être calculée à un niveau d'agrégation à partir des lois marginales, ou bien en considérant le comportement multi-échelle à l'aide des lois marginales conjointes à plusieurs Δ [11, 46].

• **Résultat de détection.** Pour la trace de l'attaque I (DDoS en UDP flooding par IPERF) on montre sur la figure 10, le comportement de ces distances avant, pendant puis après l'attaque. L'anomalie est visible à travers l'augmentation de la distance D_α ou des divergences de Kullback. Elle n'est cependant pas visible en D_β, ce qui est attendu : un changement de forme en β serait représentatif d'un forte variation du débit seul. Ici cependant, même si le débit varie pendant l'attaque (l'attaque représente 17% du trafic global), ce sont principalement les corrélations dans le trafic légitime qui changent avec l'attaque. Il faut donc observer les changements de corrélations, à l'aide des $\alpha(\Delta)$. Les analyses faites ici utilisent une durée T de 1 minute pour estimer les paramètres. La référence est fixée en utilisant 15 minutes de trafic pris quelque temps avant l'anomalie (usuellement 30 min. avant). En variant alors le choix du seuil, on peut obtenir des courbes opérationnelles de récepteur (COR ; voir [11]), ou bien se contenter d'établir un taux de détection de l'anomalie en ayant donné a priori un taux de fausse alarme acceptable. À titre d'exemple, on donne le taux de détection attendu après une minute d'observation pour un taux de fausse alarme toléré de 10% ou de 20%. Pour quelques anomalies, d'intensités très différentes, le taux de bonne détection empirique est indiqué en tableau III. Les résultats pour des temps d'alerte courts, ici 1 minute, sont déjà satisfaisants.

Si on veut comparer ces résultats à ceux travaillant avec des données netflow souvent agrégées à 5 mi-

nutes [7, 31], la méthode peut encore gagner beaucoup en sensibilité en combinant les alertes sur plusieurs minutes consécutives de trafic. Une autre manière d'améliorer d'un ordre de grandeur les performances de détection de cette méthode est de filtrer au préalable le traffic par des méthodes de sketch (filtrage pseudo-aléatoire du trafic par des fonctions de hachage) [29]. En combinant les sketchs aux modèles Gamma-farima, la procédure de détection présentée arrive à des probabilités de détection très bonnes, ainsi qu'il est montré dans [1]. Notons enfin que la seule surveillance de la moyenne et la variance de X_Δ en fonction de Δ ne permet pas de détecter les anomalies que nous avons étudiées. De plus, cela ne pourrait pas permettre de discriminer les divers types d'anomalies, par exemple DDoS et FC.

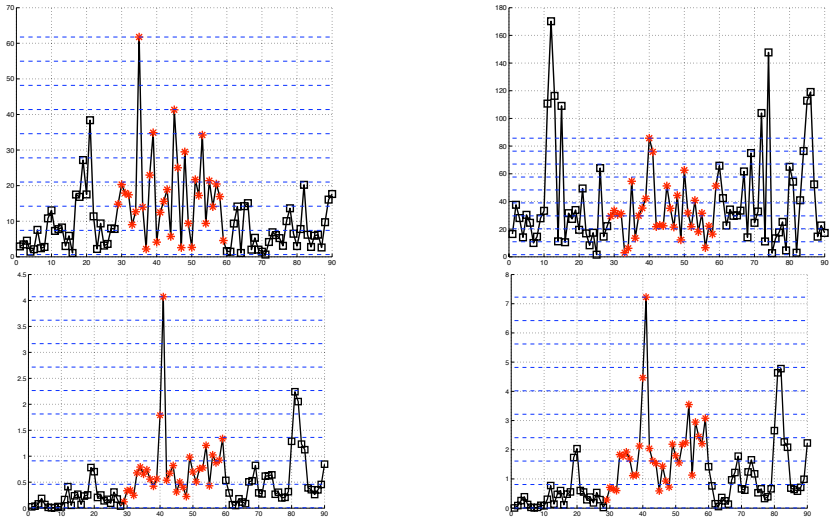

FIG. 10: En haut : distance quadratique moyenne (DQM). DQM calculée sur $\alpha(\Delta)$ à droite, et $\beta(\Delta)$ à gauche, sur des fenêtres successives (d'une minute). Les fenêtres correspondant à l'attaque (I) sont marquées par des astérisques, celles correspondants au trafic normal par des carrés. **En bas : divergences de Kullback.** À gauche, $K_D(l)$ pour l'échelle $j = 4$, à droite pour l'échelle $j = 7$, estimées sur des tranches successives d'une minute. ***Mean Quadratic Distance (DQM) (top)*** *computed on* $\alpha(\Delta)$ *(right), and* $\beta(\Delta)$ *(left) on 1 minute sliding windows. Values are shwon as asterisks during the attack (I), and squares for regular traffic conditions.* ***Kullback divergences (bottom).*** $K_D(l)$ *computer at scale* $j = 4$ *(left) and* $j = 7$ *(right), estimated on 1 minute sliding windows.*

	$P_{fa} = 10\%$			$P_{fa} = 20\%$		
	D_α	$K_{j=4}$	$K_{j=7}$	D_α	$K_{j=4}$	$K_{j=7}$
I	51	25	35	64	64	67
III	48	74	70	58	93	83
G	93	93	93	96	93	93

TAB. III: Taux de détection. Pour trois attaques de DDoS d'illustration, nous donnons les probabilités de détection empiriques obtenues sous des taux de fausse alarme de 10 % (à gauche) ou de 20 % (à droite) pour les diverses distances proposées. Ces probabilités ont été obtenues en lisant la probabilité de détection sur les courbes COR établie expérimentalement en balayant tous les seuils possibles (courbes non montrées ici) [11]. ***Detection rates.*** *For 3 DDoS attacks, we show the experimental detection probabilities obtained for a given false alarm probability of 10 % (left) or 20 % (right), for the various distances proposed here. The probabilities are obtained by comparison with all the possible threshold, so as to obtain the ROCs (as in [11]).*

IV.4 Flash Crowd

Un autre intérêt de formuler la détection d'anomalie à partir du modèle Gamma-farima proposé, est la possibilité de réduire le nombre de faux positifs en cas d'augmentation de trafic pour des raisons d'anomalies légitimes de type Flash Crowd. Il est même possible de détecter séparément et d'identifier les anomalies

légitimes et les anomalies illégitimes. L'étude menée ici porte sur les anomalies de type Flash Crowd et s'intéresse à ce que fournit le modèle et la méthode de détection lors d'un tel événement.

Les courbes de droite des figures 7 et 8 illustrent le diagramme log-échelle et les distributions $\Gamma_{\alpha,\beta}$, validant l'adéquation d'un modèle Gamma-farima pour du trafic en présence d'une Flash Crowd (FC) et ce pour un large ensemble de niveaux d'agrégation. Pour les lois marginales, les formes des courbes $\alpha(\Delta)$ et $\beta(\Delta)$ observées pendant l'événement ne s'écartent pas de façon significative de celles du trafic normal. Quelques écarts existent pour les grandes valeurs de Δ (de $0,5$ à 1 s) et cette différence de comportement se remarque aussi sur les diagrammes log-échelles.

Sur la figure 7, on constate que le diagramme log-échelle révèle un changement des corrélations dans la trafic. Pour les octaves $j = 8$ à $j = 10$, i.e., pour les échelles de temps allant de 250 ms à 1 s, un fort pic d'énergie apparaît (un tel pic n'ayant jamais été observé pour du trafic régulier). Notons que le processus farima complet (les courbes ne sont pas présentées par manque de place) ne peut représenter les corrélations à temps courts (en plus de la LRD et ce pic d'énergie) qu'en augmentant l'ordre des parties ARMA du modèle (ici d'ordre 1). Notons également que le paramètre de LRD d, lorsqu'il est estimé pour des octaves supérieures à celles correspondant au pic d'énergie ne s'écarte pas significativement des valeurs estimées avant et après la FC. On ne peut donc pas se contenter de caractériser la Flash Crowd comme une modification de LRD dans la série : son impact est de changer globalement le spectre (tel qu'estimé par le diagramme log-échelle), principalement aux échelles de temps intermédiaires.

• **Perpectives sur la détection d'anomalies.** Ces constations nous indiquent alors qu'une anomalie légitime de type Flash Crowd ne sera pas détectée par la méthodologie de détection proposée plus haut. En effet, la différence de comportement observée pour les $\alpha(\Delta)$ entre la situation d'attaque par DDoS et de FC a pour conséquence que la distance $D_\alpha(l)$ calculée localement entre les paramètres de référence et les paramètres estimés sur chaque fenêtre d'une minute ne montre pas d'augmentation pendant la FC. Notons que la FC n'intègre pas de mécanisme tendant à empêcher le phénomène « 0 paquet par fenêtre » contrairement à l'attaque DDoS et c'est une raison pour laquelle les paramètres des lois marginales ont la même évolution lors d'une FC que pour du trafic normal.

Un développement de la méthode de détection serait de construire un détecteur sur une distance spectrale locale sur les diagrammes log-échelles, qui pourrait (contrairement aux distances D_α et KD proposées) détecter les anomalies de type FC sans être déclenché par les attaques de DDoS. En perspective donc, une méthode complète de détection et identifications de diverses anomalies (légitimes ou non) est en développement en se fondant sur le modèle et les principes décrits ici.

V Conclusions et travaux futurs

Dans cet article, nous avons introduit un processus non gaussien dépendant à long terme, le processus $\Gamma_{\alpha,\beta}$-farima(P,d,Q) pour modéliser les statistiques de premier et second ordre du trafic des réseaux d'ordinateurs. Nous avons proposé des procédures d'estimation des paramètres correspondants. Nous avons montré sur un grand nombre de trafics standards de référence qu'il constitue un modèle à la fois pertinent et versatile et ce pour un grand nombre de niveaux d'agrégation Δ. Ses paramètres évoluant régulièrement avec Δ fournissent une caractérisation statistique multirésolution du trafic régulier. Nous avons également montré que des écarts par rapport à ces comportements de référence (selon Δ) nous permettent de distinguer des trafics avec ou sans anomalie, et aussi de déterminer si les anomalies sont légitimes (flash crowds) ou illégitimes (attaque DDoS). Nous avons également proposé des procédures de détection d'attaques de DDoS. Celles-ci sont intrinsèquement multirésolution (elles reposent sur les analyses conjointes du trafic agrégé à plusieurs niveaux) et consistent à seuiller des distances calculées entre une fenêtre d'observation courante et une référence.

Ce modèle et les méthodes de détection d'attaques ont été validés expérimentalement sur de nombreuses traces de trafic normal et contenant des anomalies. Ces traces comprennent des traces publiques ainsi que des traces produites par nous mêmes dans le cadre de METROSEC, en particulier des traces contenant des anomalies comme des flash crowds ou des attaques de DDoS. Ces traces ont été produites sur une plate-forme expérimentale distribuée, dont les sites sont interconnectés par RENATER. Sur cette plate-forme maîtrisée, les conditions expérimentales sont reproductibles. Nous avons ainsi pu réaliser des campagnes

d'attaques au cours desquelles nous avons pu faire varier les intensités et caractéristiques des attaques de manière contrôlée. Nous disposons donc aujourd'hui d'une base de traces de trafics réguliers et de trafics contenant des anomalies documentées. Toute la validation du modèle de trafic et des procédures de détection d'attaques que nous avons proposés repose sur l'exploitation de cette base de traces de trafics.

Ce travail sera poursuivi, d'une part, par la réalisation de nouvelles campagnes d'attaques mettant en jeu d'autres intensités, protocoles, caractéristiques ou mécanismes et d'autre part, par le développement des procédures de détection (détermination automatique des seuils pour une probabilité de fausse alarme fixée (usage de technique dite de *bootstrap*), usage d'autres distances, exploitation renforcée de l'aspect multirésolution. Enfin, on explorera la possibilité de descendre la durée des fenêtres de détection en deçà de la minute, celle-ci faisant l'objet d'une dégradation du compromis détection correcte/fausse alarme. A terme, nous tracerons les contours d'un prototype d'IDS basé sur les principes énoncés dans cet article.

Remerciements

Les auteurs remercient le CRI de l'ENS Lyon, le CIUPPA de l'IUT de Pau et L. Bernaille du LIP6, Paris 6, pour leur aide dans la collecte de données de trafic et dans la conduite des expérimentations d'attaques. Ils remercient aussi tous les collègues qui ont gracieusement accepté de prendre part à l'expérimentation de foule subite étudiée dans cet article. Enfin, ils remercient ceux qui rendent leurs traces de trafic publiques (Bellcore, LBL, UNC, Auckland Univ, Univ North Carolina, CAIDA). Ils remercient spécialement S. Marron, F. Hernandez-Campos et C. Park de l'UNC, USA, D. Veitch et N. Hohn du CubinLab, University of Melbourne, Australie pour avoir pré-formaté certaines des séries temporelles utilisées ici. Ce travail a été rendu possible grâce au support financier du MNRT dans le cadre du programme ACI *Sécurité et Informatique* 2004, qui soutient le projet METROSEC.

Références

[1] (P.) ABRY, (P.) BORGNAT, and (G.) DEWAELE. Sketch based anomaly detection, identification and performance evaluation. In *Workshop on Internet Measurement Technology and its Applications to Building Next Generation Internet, in EEE-CS & IPSJ SAINT 2007)*, January 2007.

[2] (P.) ABRY and (D.) VEITCH. Wavelet analysis of long-range dependent traffic. *IEEE Trans. on Info. Theory*, 44(1) :2–15, January 1998.

[3] TFN2K An analysis. http ://packetstormsecurity.org/distributed/TFN2k_Analysis-1.3.txt.

[4] (A.) ANDERSEN and (B.) NIELSEN. A Markovian approach for modelling packet traffic with long range dependence. *IEEE journal on Selected Areas in Communications*, 5(16) :719–732, 1998.

[5] IPERF The TCP/UDP bandwith Measurement Tool. http ://dast.nlanr.net/Projects/Iperf/.

[6] (C.) BARAKAT, (P.) THIRAN, (G.) IANNACCONE, (C.) DIOT, and (P.) OWEZARSKI. A flow-based model for internet backbone traffic. In *ACM/SIGCOMM Internet Measurement Workshop*, pages 35–47, New York, NY, USA, 2002. ACM Press.

[7] (P.) BARFORD, (J.) KLINE, (D.) PLONKA, and (A.) RON. A signal analysis of network traffic anomalies. In *ACM/SIGCOMM Internet Measurement Workshop*, pages 71–82, Marseille, France, November 2002.

[8] (M.) BASSEVILLE. Distance measures for signal processing and pattern recognition. *Signal Processing*, 18 :349–369, 1989.

[9] (J.) BERAN. *Statistics for Long-memory processes*. Chapman & Hall, New York, 1994.

[10] (P.) BORGNAT, (N.) LARRIEU, (P.) ABRY, and (P.) OWEZARSKI. Détection d'attaques de "déni de services" : ruptures dans les statistiques du trafic. In *Colloque GRETSI-2005*, pages 323–326, Louvain-la-Neuve, Belgique, September 2005.

[11] (P.) BORGNAT, (N.) LARRIEU, (P.) OWEZARSKI, (P.) ABRY, (J.) AUSSIBAL, (L.) GALLON, (G.) DEWAELE, (K.) BOUDAOUD, (L.) BERNAILLE, (A.) SCHERRER, (Y.) ZHANG, and (Y.) LABIT. Détection d'attaques de dénis de service par un modèle non gaussien multirésolution. In *Conf. Francophone d'Ingénieurie des Protocoles, CFIP-2006*, pages 303–314, November 2006.

[12] (J.) BRUTLAG. Aberrant behavior detection in time series for network monitoring. In *USENIX System Administration Conference*, pages 139–146, New Orleans, December 2000.

[13] (C-M.) CHENG, (H.T.) KUNG, and (K-S.) TAN. Use of spectral analysis in defense against DoS attacks. In *IEEE Globecom*, volume 3, pages 2143–2148, Taipei, Taiwan, 2002.

[14] (J.) CLEARY, (S.) DONNELLY, (I.) GRAHAM, (A.) MCGREGOR, and (M.) PEARSON. Design principles for accurate passive measurement. In *Passive and Active Measurements*, pages 1–7, Hamilton, New Zealand, apr 2000.

[15] (P.) DOUKHAN, (G.) OPPENHEIM, and (M.S.) TAQQU. *Long-Range Dependence : Theory and Applications*. Birkhäuser, Boston, 2003.

[16] (A.) ERRAMILLI, (O.) NARAYAN, and (W.) WILLINGER. Experimental queueing analysis with long-range dependent packet traffic. *ACM/IEEE transactions on Networking*, 4(2) :209–223, 1996.

[17] (M.) EVANS, (N.) HASTINGS, and (B.) PEACOCK. *Statistical Distributions*. Wiley (Interscience Division), June 2000.

[18] (S.) FARRAPOSO, (K.) BOUDAOUD, (L.) GALLON, and (P.) OWEZARSKI. Some issues raised by DoS attacks and the TCP/IP suite. In *SAR' 2005*, pages 297–306, Batz-sur-mer, France, June 2005.

[19] (A.) FELDMANN, (A.C.) GILBERT, and (W.) WILLINGER. Data networks as cascades : Investigating the multifractal nature of internet wan traffic. In *ACM/SIGCOMM conference on Applications, technologies, architectures, and protocols for computer communication*, pages 42–55, 1998.

[20] (M.) GROSSGLAUSER and (J.) BOLOT. On the relevance of long-range dependence in network traffic. In *ACM SIGCOMM*, pages 15–24, 1996.

[21] (G.J.) HAHN and (S.S.) SHAPIRO. *Statistical Models in Engineering*, page 88. Wiley (Interscience Division), June 1994.

[22] HPING2. http ://sourceforge.net/projects/hping2.

[23] (C.) HUANG, (M.) DEVETSIKIOTIS, (I.) LAMBADARIS, and (A.) KAYE. Modeling and simulation of self-similar Variable Bit Rate compressed video : a unified approach. In *ACM SIGCOMM*, pages 114 – 125, Cambridge, UK, August 1995.

[24] (A.) HUSSAIN, (J.) HEIDEMANN, and (C.) PAPADOPOULOS. A framework for classifying denial of service attacks. In *SIGCOMM*, pages 99–110, Karlsruhe, Germany, August 2003.

[25] (S.) JIN and (D.) YEUNG. A covariance analysis model for DDoS attack detection. In *IEEE International Conference on Communications*, volume 4, pages 1882–1886, Paris, France, June 2004.

[26] (J.) JUNG, (B.) KRISHNAMURTHY, and (M.) RABINOVICH. Flash Crowds and Denial of Service Attacks : Characterization and Implications for CDNs and Web Sites. In *International WWW Conference*, pages 293–304, Honolulu, HI, May 2002.

[27] (S.) KANDULA, (D.) KATABI, (M.) JACOB, and (A.) BERGER. Botz-4-sale : surviving organized DDoS attacks that mimic Flash Crowds. In (A.) VAHDAT and (D.) WETHERALL, editors, *USENIX' NSDI'05*, Boston, MA, May 2005.

[28] (T.) KARAGIANNIS, (M.) MOLLE, (M.) FALOUTSOS, and (A.) BROIDO. A nonstationary Poisson view of the internet traffic. In *INFOCOM*, volume 3, pages 1558–1569, 2004.

[29] (B.) KRISHNAMURTY, (S.) SEN, (Y.) ZHANG, and (Y.) CHEN. Sketch-based change detection : Methods, evaluation, and applications. In *ACM IMC*, pages 234–247, October 2003.

[30] laasnetexp.fr. http ://www.laas.fr/ owe/laasnetexp.fr/laasnetexp.fr.htm.

[31] (A.) LAKHINA, (M.) CROVELLA, and (C.) DIOT. Diagnosing network-wide traffic anomalies. In *SIGCOMM*, pages 219–230, August 2004.

[32] (W.E.) LELAND, (M.S.) TAQQU, (W.) WILLINGER, and (D.V.) WILSON. On the self-similar nature of ethernet traffic (extended version). *ACM/IEEE transactions on Networking*, 2(1) :1–15, February 1994.

[33] (L.) LI and (G.) LEE. DDoS attack detection and wavelets. In *International Conference on computer communications and networks*, pages 421– 427, August 2003.

[34] (L.) LJUNG. *System identification : theory for the user*, chapter 10.2. PTR Prentice Hall, 1999.

[35] (B.) MELAMED. An overview of TES processes and modeling methodology. In *Performance/SIGMETRICS Tutorials*, pages 359–393, 1993.

[36] (D.) MOORE, (G.M.) VOELKER, and (S.) SAVAGE. Inferring internet denial-of-service activity. In *Usenix Security Symposium*, pages 9–22, 2001.

[37] (I.) NORROS. On the use of fractional Brownian motion in the theory of connectionless networks. *IEEE journal on Selected Areas in Communications*, 13(6) :953–962, 1995.

[38] (P.) OWEZARSKI, (N.) LARRIEU, (L.) BERNAILLE, (W.) SADDI, (F.) GUILLEMIN, (A.) SOULE, and (K.) SALAMATIAN. Distribution of traffic among applications as measured in the french metropolis project. *Annals of Telecommunication, Special issue on Analysis of traffic and usage traces on the Internet - From network engineering to sociology of uses*, to appear, 2007.

[39] (K.) PARK, (G.) KIM, and (M.) CROVELLA. On the relationship between file sizes, transport protocols, and self-similar network traffic. In *International Conference on Network Protocols*, pages 171–180, Washington, DC, USA, 1996. IEEE Computer Society.

[40] (K.) PARK and (W.) WILLINGER. Self-similar network traffic : An overview. In Kihong PARK and Walter WILLINGER, editors, *Self-Similar Network Traffic and Performance Evaluation*, pages 1–38. Wiley (Interscience Division), 2000.

[41] (V.) PAXON and (S.) FLOYD. Wide-area traffic : The failure of Poisson modeling. *ACM/IEEE transactions on Networking*, 3(3) :226–244, June 1995.

[42] (V.) PAXSON. Bro : a system for detecting network intruders in real-time. *Computer Networks Journal*, 31(23-24) :2435–2463, 1999.

[43] METROSEC project. http ://www.laas.fr/METROSEC.

[44] QoSMOS Traffic Designer. http ://www.qosmos.net.

[45] (A.) SCHERRER and (P.) ABRY. Marginales non gaussiennes et longue mémoire : analyse et synthèse de trafic Internet. In *Colloque GRETSI-2005*, Louvain-la-Neuve, Belgique, September 2005.

[46] (A.) SCHERRER, (N.) LARRIEU, (P.) OWEZARSKI, (P.) BORGNAT, and (P.) ABRY. Non-gaussian and long memory statistical characterisations for internet traffic with anomalies. *IEEE Transaction on Dependable and Secure Computing*, 4(1), January 2007.

[47] (M.) TAQQU, (V.) TEVEROSKY, and (W.) WILLINGER. Is network traffic self-similar or multifractal ? *Fractals*, 5(1) :63–73, 1997.

[48] The DoS Project's "trinoo" distributed denial of service attack tool. http ://staff.washington.edu/dittrich/misc/trinoo.analysis.

[49] (H.S.) VACCARO and (G.E.) LIEPINS. Detection of anomalous computer session activity. In *IEEE Symposium on Security and Privacy*, pages 280–289, Oakland, California, May 1989.

[50] (D.) VEITCH and (P.) ABRY. A wavelet based joint estimator of the parameters of long-range dependence. *IEEE Trans. on Info. Theory special issue on "Multiscale Statistical Signal Analysis and its Applications"*, 45(3) :878–897, April 1999.

[51] (D.) VEITCH and (P.) ABRY. A statistical test for the time constancy of scaling exponents. *IEEE Transactions on Signal Processing*, 49(10) :2325–2334, October 2001.

[52] (N.) YE. A Markov chain model of temporal behavior for anomaly detection. In *Workshop on Information Assurance and Security*, pages 171–184, West Point, NY, June 2000.

[53] (J.) YUAN and (K.) MILLS. DDoS attack detection and wavelets. Technical report, National Institute of Standards and Technology, 2004.

[54] (Z.) ZHANG, (V.) RIBEIRO, (S.) MOON, and (C.) DIOT. Small time scaling behavior of internet backbone traffic : an empirical study. *INFOCOM*, 3 :1826–1836, March 2003.